PROJECT MANAGEMENT IN THE IMPLEMENTATION OF GENERAL DATA PROTECTION REGULATION (GDPR)

Ivan Todorović[1], Stefan Komazec[2], Đorđe Krivokapić[3], Danilo Krivokapić[4]
[1,2,3]*Faculty of Organizational Sciences, University of Belgrade, Serbia*
[4]*SHARE Foundation, Serbia*

Abstract: Technology development and digitalization have reshaped business models and made data one of the key resources in business ecosystem. Organizations have become more focused on gathering and processing personal data for the purpose of gaining competitive advantage and profit. Consequently, the importance of personal data protection has significantly grown, since one of the fundamental civil rights, the right of privacy, has become more jeopardized than ever before. This caused major changes in the European Union (EU) legislation related to personal data protection, which resulted in the introduction of General Data Protection Regulation (GDPR). The new regime significantly increases the protection of EU data subjects, but also demands all controllers and processors of personal data to adjust their business in order to avoid huge fines for non-compliance. This paper deals with project management in the process of implementing GDPR provisions.

Key words: General Data Protection Regulation, GDPR, data protection, personal data, privacy, EU legislation, compliance, project management

1. INTRODUCTION

Digitalization triggered off a new industrial revolution which is based on data, primarily due to a significant advancement in terms of performance of processors and expansion of availability and use of technology (COM (2014) 442 final). Therefore many stakeholders have become enabled to collect personal data of their interest groups and thus base their business models according to the information collected. Personal data have always been present in a certain form, but the development of technology and a wider application of primarily mobile communication and social networks made them available in a much easier and faster manner to all those who provide services by using these channels (Schwab, Marcus, Oyola, Hoffman, & Luzi, 2011). Through their everyday activities, the users of information and communication technologies make their personal data available to different entities which provide services via the Internet, and yet they are not entirely aware of all possible purposes and manners of further processing of those data. This may cause the violation of privacy, which is one of the fundamental human rights (Gounalakis, 2000). The right to the protection of personal data is a legal legacy of privacy, but it is still an autonomous right in relation to privacy (Bygrave, 2014). Certain authors emphasize that the protection of privacy involves limitations regarding data access, whereas the protection of personal data entails ensuring transparency of their processing (Heisenberg, 2005; Blume, 2012; Fan, 2015). Unauthorized processing of personal data may jeopardize identity, reputation, and even safety of persons to which they refer, thus protection of personal data in legal sense overcomes the protection of privacy itself (De Andrade, 2010). Due to all of this, the issue of protection of personal data will have an increasingly bigger importance in future (Purtova, 2011).

2. REGULATIONS IN THE FIELD OF PERSONAL DATA PROTECTION

General regulation regarding the protection of personal data (Regulation (EU) 2016/679, 2016, i.e. General Data Protection Regulation, hereinafter GDPR) is a new legislative

Corresponding author. Email: ivan.todorovic@fon.bg.ac.rs
ISSN 2560-4961(online)

doi: 10.18485/epmj.2018.8.1.7

framework prescribing the way of using personal data of the European Union (EU) citizens, the provisions of which are mandatory to all organizations which process their personal data in any way, regardless of the fact whether their official location is in the EU territory or not (Tankard, 2016). This Regulation entered into force on 25 May 2018, with a goal of replacing the Directive on Data Protection 1995 which was in force until then (Directive 95/46/EC) and thus to create a unique legal instrument directly applicable in all countries of the EU and beyond (Zarsky, 2016). Namely, while this Directive was in force, there was no compliance of the laws on protection of personal data among the EU member states, because it allowed them to adopt local regulations (González, Echevarría, Morales, & Ruggia, 2016). The GDPR has now become a substitute for all different ways in which the previous Directive was implemented and took into account new technologies which were not covered in the Directive. In this manner, the GDPR introduced new, more comprehensive and uniform rules regarding the usage and protection of personal data (Albrecht, 2016).

As mentioned before, the GDPR will not apply exclusively to organizations dealing with personal data processing which have their offices in some EU states, instead the application field of this Regulation expands outside the EU borders – to organizations which offer goods or services to the EU citizens or monitor the behavior of citizens if this behavior occurs in the territory of the EU (Krivokapić, Krivokapić, Todorović, & Komazec, 2018). This is especially important issue for emerging countries, since they open their economies, offer long-term investment opportunities for foreign investors and increase market activities with other countries (Jednak, 2017), which most probably includes personal data processing. Therefore, every organization doing its business online or every organization which processes personal data of the EU citizens for the needs of conducting business, will be required to conduct the project of implementation of the GDPR provisions as soon as possible and to ensure compliance of its business with six basic GDPR principles (GDPR, 2016 – Article 5):

(1) Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject, meaning:
   a) processing must occur only if there is a legal basis and the respect of all regulations applied to the processing,
   b) controllers and processors must always keep in mind the vital interests of the data subject or of another natural person to which collected data refers,
   c) data subjects have the right to know what is happening with the data from the moment of their collection.
(2) Purpose limitation – data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
(3) Accuracy – data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
(4) Minimization – personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
(5) Integrity and confidentiality – data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate:
   a) technical measures – access authorization, pseudonymization, anonymization;
   b) organizational measures – staffing, involving DPO.
(6) Storage limitation – data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer

> periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, under certain conditions.

The main problem is that there is no previous experience in such compliance projects, since the regulation came into the force this year. This may cause difficulties for many organizations, since one of the major issues for knowledge management in a project environment is the poor project success analysis and the lack of proper documentation on the results of the previous projects (Todorović, Petrović, Mihić, Obradović, & Bushuyev, 2015). For this reason we try to identify most important changes in personal data management legislation and to propose key roles and activities in the project of their implementation.

The existing legislative framework based on Directive 95/46/EC identifies two roles in the processing of personal data. The controller is an entity determining the purpose and manner of data processing, while the processor is an entity which processes data at the request of the controller and for the specific purpose of the controller. The previous Directive placed all liability regarding personal data protection on the controller, whereas the processor was not liable provided that this entity followed the provisions of the agreement with the controller (Krivokapić, Krivokapić, Todorović, & Komazec, 2016). In other words, the processor had to make a request that the controller ensured the data processing was in line with the law, as well as to envisage all possible scenarios and define agreement provisions accordingly, in order to ensure the protection of personal data.

Under the influence of technology, the new Regulation stipulates additional aspects of privacy and protection and defines additional rights of data subjects whose data are processed, and thus it largely increases the obligations of organizations processing personal data (Blume, 2015). Furthermore, the GDPR specifies two roles in personal data processing and defines them in the same manner, however, it increases the liability of the processor, although it is still the controller that has more obligations than the processor. Namely, the GDPR clearly states that all controllers and processors must conduct adequate technical and organizational measures in order for the Regulation provisions to be applied and thus it extends the scope of organizations where it is necessary to implement the GDPR provisions. Provided that the regulations are not respected, the maximum fines reach 20 million EUR or 4% of an annual organization turnover, which places an additional importance of a timely compliance of business with the new Regulation (Voigh, & von dem Bussche, 2017).

3. COMPLIANCE WITH THE GDPR

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity regarding the rights and freedoms of natural persons, the controller will implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation (GDPR, 2016). This entails a set of measures, meaning that in every organization which applies the GDPR it is necessary to achieve the compliance of business processes and internal organizations with the provisions of the new Regulation (De Guise, 2017).

Controllers and processors are obligated to appoint a data protection officer (DPO) in the following cases (Lambert, 2016):

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data relating to criminal convictions and offences.

The GDPR does not prescribe specific qualifications for performing the function of the data protection officer, but it does state that it is necessary for the employee to have expert

knowledge regarding legislation and practice in the field of data protection, as well as the ability to perform the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant GDPR;
- to monitor compliance of the controller or processor with the Regulation, with other Union or Member State data protection provisions;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to raise the awareness on the importance of GDPR and making the staff equipped to participate in processing activities;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing.

All controllers must keep records on personal data processing and to report them to the supervisory authorities. Keeping these records on personal data processing and their official registration at the Commissioner for Personal data Protection is an obligation which is also prescribed in the current Law in Serbia, too. However, research has shown that only few organizations in Serbia follow these regulations (Krivokapić, et al., 2016). The GDPR stipulates slightly less obligations when it comes to this issue, and so it prescribes only the obligation of keeping these records at organizations with more than 250 employees, with certain exceptions for smaller controllers and processors. Therefore, it is possible to expect amendments of domestic legislation in order to ensure the compliance with the new EU regulation, but even in this case keeping the records will remain mandatory for bigger controllers and processors.

Another organizational measure referring to the application of the GDPR provisions is a risk assessment in terms of personal data processing in order to prevent personal data breach. According to the GDPR, personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

According to the principles of the Working Party 29[1] there are three types of personal data breach:

1. "Confidentiality breach" - where there is an unauthorized or accidental disclosure of, or access to, personal data.
2. "Integrity breach" - where there is an unauthorized or accidental alteration of personal data.
3. "Availability breach" - where there is an accidental or unauthorized loss of access to, or destruction of, personal data.

The GDPR does not prescribe a mandatory methodology for the risk assessment in terms of personal data processing activity. However, based on observing the core provisions, it can be concluded that the methodological framework could contain: the definition of processing and the context of processing, understanding and assessment of the impact of processing, definition of possible threats and the assessment of their feasibility, as well as the very risk assessment representing the combination of potential negative impact and the probability of risk occurrence.

In case there is a personal data breach, the controller will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If there is a probability that the

[1] Article 29 Working Party, set out in Article 29 of the Data Protection Directive was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. One of its main stated missions was to provide expert advice to the States regarding data protection by issuing numerous guidelines and opinions. After coming into force of GDPR, it has been replaced by the European Data Protection Board (EDPB) with same purpose.

personal data breach will cause a great risk for rights and freedoms of natural persons, then the controller will without undue delay also notify the subjects to which the data refer about the personal data breach. This obligation of formally notifying competent bodies belongs only to the controller. However, the processor must inform the controller as soon as an incident occurs, provide all the information necessary for producing an official notification and keep records on all incidents related to security. The official notification must fulfill at least the following conditions:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

In addition to this, organizations outside the EU which conduct the data processing of the EU citizens must appoint their representatives in the EU when the processing activities are related to offering goods or services to subjects to which the data refers. This should be ensured regardless of the fact whether the subject is to make a payment or only receive information, or in cases of monitoring of the EU citizens behavior if that their behavior occurs within the EU. The representative must be located in one of the EU member states where there are subjects whose personal data is processed. The controller or processor mandates the appointed representative to be addressed by all supervisory bodies and subjects to which data refers, on all issues related to processing. It is important to notice that appointing the representative of the controller or processor does not influence legal actions which may be taken against the very controller or processor. The appointed representative should be the object of the process of ensuring the application of legislation in case the controller or processor does not follow the regulations.

Considering the fact that today almost all personal data processing organizations keep the data in the electronic form and use different types of software tools for data processing, it is necessary to take adequate technical measures in order to ensure data protection. Therefore, it is necessary to conduct pseudonymization and the encryption of personal data, ensure permanent confidentiality,comprehensiveness, availability and resistance of all systems and services of data processing as well as to ensure a timely re-establishment of personal data availability and their access in case there is a physical or a technical incident. The need for the access to personal data may be the need of different interest groups such as employees, bodies of authority, legal entities with which there are signed agreements referring to business cooperation, natural persons about whom data is collected, and even the public in certain situations. Related to this, the controller is obligated to disable the unauthorized access to the segments of system which contain personal data, digitally or physically, to limit the use, that is, the processing of data for only specific purposes determined beforehand, to disable the excessive data use (quantitative and qualitative), and to establish a mechanism for the deletion of unnecessary system data. Therefore, the GDPR stipulates that the information systems used for personal data processing must be projected so as to meet two basic principles:

1) Privacy by Design;
2) Privacy by Default.

This means that the controller will, both at the time of the determination of the means for processing and at the time of the processing itself, implement data-protection principles in an effective manner and integrate the necessary safeguards into the processing in order to meet the requirements of GDPR and protect the rights of data subjects. Furthermore, these measures will ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures

shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons (GDPR, 2016). The system of users' roles is to ensure an adequate level of access of all interest groups after their authentication. The authorization should enable them to access only the personal data for which there is a purpose of processing.

In addition to the regular backup of the very personal data in order to ensure their availability in case of any technical incident, it is also necessary to store the information on the processing activities referring to them. Logs should provide digital evidence in case of any personal data breach and the violation of privacy of persons whose data is processed. Additionally, these measures will have to be regularly tested and updated (Venkataramanan, & Shriram, 2016).

Apart from technical measures referring to software solutions, there are also stipulated measures including hardware components. Namely, it is necessary to map the resources and produce a catalogue of IT equipment used for accessing databases containing personal data, in order to conduct a risk assessment for each of them. Based on the assessment results, adequate measures of prevention should be taken and there should be a defined plan of solutions in case risks occur.

It is recommended that the personal data protection within an organization is regulated by passing an adequate internal document. Regulating the field of personal data protection through internal documents is a good practice in many developed countries. Such document should regulate issues referring to the data processing procedure, protection of personal data, informing subjects on the manner of realization of rights in terms of data processing and the necessary measures of data protection, the access to personal data and liability related to their unlawful processing and use, as well as keeping the records on processing every collection of data (Krivokapić, Krivokapić, Todorović, Komazec, Petrovski, & Ercegović, 2016).

4. KEY ROLES IN THE PROJECT OF GDPR IMPLEMENTATION

Taking into account a wide scope of aspects covering the basic principles of GDPR, it is clear that for their implementation it is necessary to have an interdisciplinary team capable of primarily understanding the regulatory framework and the sense of very general legal norms which must be applied to individual situations in various business fields. The team must be capable of assessing whether and to what extent it is applied to the organization in which the project is conducted, and then, based on the analysis of the present situation, to observe all current aspects of the lack of compliance, define directions for making the business compliant with the new regulatory framework and finally propose organizational and technical measures to ensure a full application of regulations in all aspects of business of an organization. With that in mind, we can define three key roles in a project team:

(1) Expert for legal issues,
(2) Expert for organizational issues,
(3) Expert for technical issues and information security.

Depending on the size and the scope of work of an organization, the project team may have more members who will be divided into three groups at the highest level of hierarchy, according to the criteria of competences they have. However, each project team should have at least three given members. It is important to note that the support of the top management of an organization to the project team is crucial for a successful realization of such project, considering that exceptional business skills and knowledge of business models are necessary for a success.

5. KEY ACTIVITIES IN THE PROJECT OF GDPR IMPLEMENTATION

The following diagram shows a proposal of main stages and affiliated activities within the project of implementation of GDPR and compliance of business with its provisions (Todorović, Komazec, & Krivokapić, 2018).

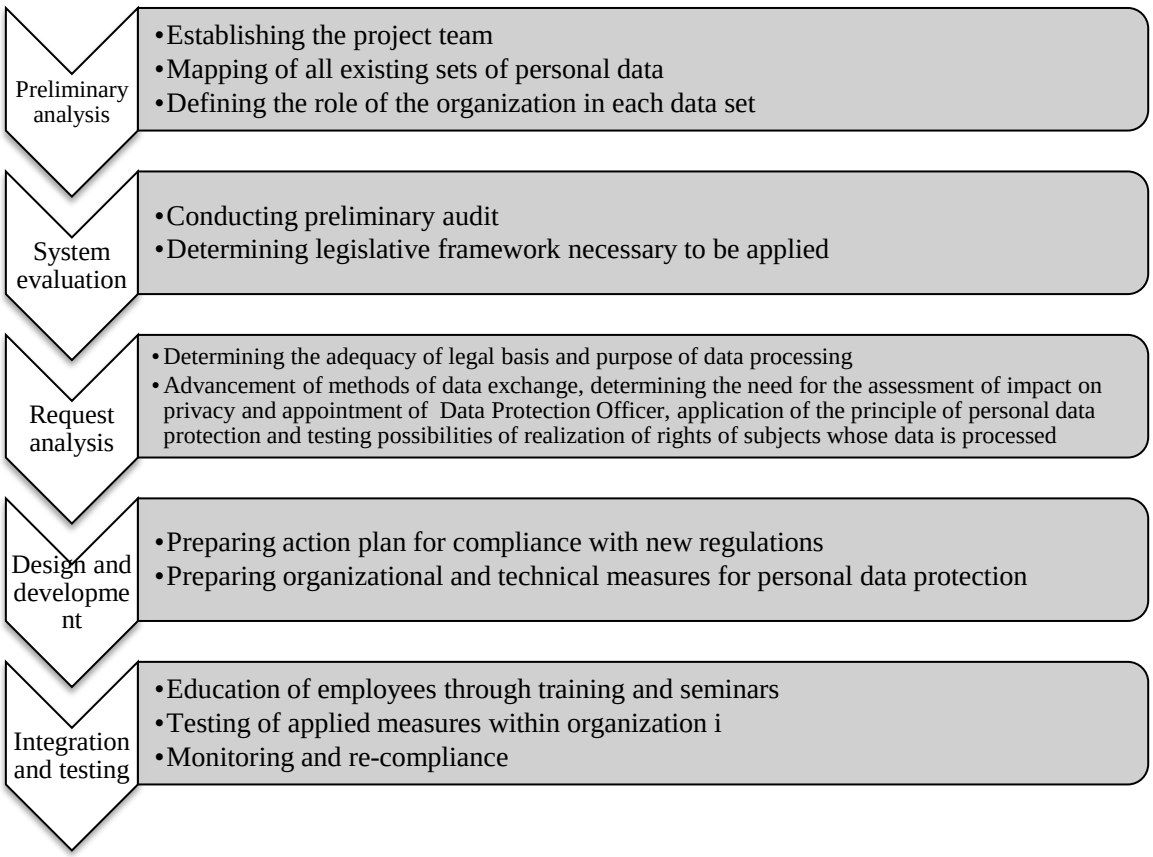

Figure 1: Key activities and stages in the project of making business compliant with GDPR

For a successful beginning and conducting the GDPR implementation, it is necessary to bring the importance of this compliance into awareness, firstly at the highest management levels. If the top management does not understand the significance and does not provide support, it is very likely that the compliance will be a failure due to the influence on the organization which is often rather substantial and thus it is demanding in terms of resources, too.

When conducting 'Preliminary analysis', after a project team is established, it is necessary to map all the personal data collections within the organization. At this point, a special attention could be paid to collecting information on types of data, sources, competent person, purpose and business processes within which the data are used. In order to lessen the liability and manage the implementation expenses, this would be a precise moment to remove the personal data which are not necessary for conducting business. It is recommended that the organization removes all the personal data collected by then which are not crucial for its conducting business. The data may be destroyed or anonymized so as to be used later on for statistical purposes. The analysis of remaining collections and data processing would determine the role of the organization, that is, whether it is a controller or a processor. It should be kept in mind that one data collection may require two processing activities and the organization may thus appear in two different corresponding roles.

The 'System evaluation' involves the 'state analysis', in order for the request analysis to be conducted later on. This includes determining the legal basis for data processing until that time, the existence of specific purposes and types of processing (profiling, behavior monitoring) and processing special types of personal data. Additionally, internal documents are collected and analyzed, too. These documents may refer to managing data, mapping of the information system and data flows, relations with processors and data storage time limitation. After this, based on the data on legal status of the organization and characteristics of data processing, it is determined to which processing the GDPR is applied, as well as which national legislation

and other regulatory specificities follow the GDPR application. This information is necessary.

The 'state analysis' is conducted with a goal of determining the lack of compliance of the existing system with the GDPR. Firstly, the adequacy of the existing legal basis and purpose of data processing is determined, and at this point a special attention is paid to processing based on agreement and a legitimate interest, as well as the processing of special personal data and data referring to minors. Then there is consideration of optional issues appearing only with some processing activities such as: transfer of data in third party countries, conducting the impact assessment regarding the protection of personal data and appointing persons for the protection of personal data. Finally, there is a thorough analysis of the application of the personal data protection principle and testing the possibilities of realization of rights of subjects whose data are processed, taking into account that they are the core of the GDPR and that it is precisely on these issues that legal risks in practice appear most often.

After all the points of the lack of compliance are determined, it is possible to begin 'Design and development'. Firstly, the Action Plan is produced in line with principles of privacy by design & default, organizational changes are projected, restructuring the existing data flow and changes of the information systems used for personal data processing are envisaged, as well as the implementation of adequate organizational and technical measures. The Action Plan thus contains a set of specific measures, the most significant ones being: compliance of the existing and development of new internal documents and policies, production and conclusion of new contracts with processors and users, production of records on processing, risk assessment and the development of reporting procedures in crisis situations, conducting optional certifications, acceptance and implementation of self-regulatory codes of conduct and mandatory business rules. Additionally, it is necessary to restructure data flow within the information infrastructure, to implement and test the implementation of all new rights of citizens and finally to conduct an elementary audit of the compliance of the processor.

Finally, as a continuous process, it is necessary to conduct 'Integration and testing' through training of employees dealing with personal data, testing of applied measures in the organization and compliance of newly discovered lacks of compliance. Finally, it should be kept in mind that if there are any further changes in personal data processing activities, and especially when it comes to new activities connected with the processing, new purposes or new personal data, it is necessary to re-examine the established compliance model.

6. CONCLUSION

Based on the comparative analysis of GDPR and Directive 95/46/EC replaced by the GDPR and after the provisions of the new regulation were observed, there are key steps defined in terms of making businesses compliant with the new regulatory framework. Even though the GDPR introduced certain new obligations for organizations processing personal data, such as the extended liability of the processor, more precise definitions of obligations concerning technical and organizational measures, it should still be emphasized that the GDPR is based on the same principles and core rules as the Directive 95/46/EC. Therefore, in the normative sense, the GDPR entering into force is primarily an evolution and certainly not a revolution in this field, since the organizations processing personal data had numerous obligations in terms of the application of technical and organizational measures for the protection of personal data even before 25 May 2018. However, a rapid development of information and communication technologies and business models based on data, as well as numerous challenges and risks which privacy and personal data protection face, made these issues in the focus of both professional and general public, and legislators and decision makers. This is supported by the fact that within the EU institutions, the GDPR was passed in a very complex process lasting for over four years with a record number of 4,000 amendments. The biggest change resulting from the GDPR refers to the amount of stipulated fines. Namely, minor offences succumb to a maximum fine of 10,000,000 EUR, or 2% of the entire annual turnover (whichever is bigger), whereas more serious offences may be fined with a maximum

amount of 20,000,000 EUR or 4% of the annual turnover (whichever is bigger).

Considering the importance placed onto the process of passing the GDPR, we can expect that supervisory bodies in the EU will significantly strengthen the control of the organizations processing personal data. On the other hand, the amount of fines prescribed by the GDPR, which was until recently a characteristic of the field of protection of competition only, makes the disrespect of rules stipulated by the GDPR a high risk for the sustainability of business of those organizations.

With that in mind, their implementation of rules prescribed by the GDPR is a binding, but also a necessary step for all organizations processing personal data of citizens located in the EU, whether they are in the role of a controller or of a processor. GDPR stipulates obligations with a high level of generality, thus the implementation process will depend on the size of the organization and the type of data processing, but stages presented in Chapter 5 of this article are much-necessary steps in every implementation process. Key roles in the implementation process based on a necessary expertise of project team members were also determined. Further research should be directed at decomposing these basic activities and connecting their realization with experts' profiles.

After the project implementation of business with GDPR, it is necessary to ensure the process of regular testing, evaluation and assessment of effectiveness of technical and organizational measures in order to achieve the security of processing. The process of implementation of business with GDPR is in fact an endless process, because every new data base, every new purpose of personal data processing will require going through the entire process again, in order to make the business of the organization entirely compliant with GDPR and to lessen the risks of high fines.

ACKNOWLEDGEMENT

Authors' engagement on this research was partially supported by the Ministry of Education and Science of the Republic of Serbia through the Project No. 179081: Researching Contemporary Tendencies of Strategic Management Using Specialized Management Disciplines in Function of Competitiveness of Serbian Economy.

REFERENCES

Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, *2*, 287.

Blume, P. (2012). Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law, 2(3)*. pp. 130–136. DOI: https://doi.org/10.1093/idpl/ips007.

Blume, P. (2015). Data Protection and Privacy – Basic Concepts in a Changing World. *Scandinavian Studies In Law*. pp. 152-164. Retrieved from http://www.scandinavianlaw.se/pdf/56-7.pdf

Bygrave, L. A. (2014). *Data Privacy Law: an International Perspective*. Oxford University Press, Oxford, UK.

COM (2014) 442 final. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Towards a thriving data-driven economy*. Retrieved from https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:52014DC0442&from=EN

de Guise, P. (2017). *Data Protection: Ensuring Data Availability*. Taylor & Francis, UK.

de Andrade, N. N. G. (2010, August). Data protection, privacy and identity: distinguishing concepts and articulating rights. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (pp. 90-107). Springer, Berlin, Heidelberg.

DIRECTIVE 95/46/EC (1995). *Official Journal of the European Union L 281, 23/11/1995, pp. 31-50.* Retrieved from http://data.europa.eu/eli/dir/1995/46/oj

Fan, M. (2015). Private Data, Public Safety: A Bounded Access Model of Disclosure. *North Carolina Law Review, 94(1)*, pp. 161-207.

General Data Protection Regulation (2016). REGULATION (EU) 2016/679. *Official Journal of the European Union L 119*. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

González, L., Echevarría, A., Morales, D., & Ruggia, R. (2016). An E-government Interoperability Platform Supporting Personal Data Protection Regulations. *CLEI Electronic Journal, 19(2)*, p.8.

Gounalakis, G. (2000). *Privacy and the Media: A Comparative Perspective, Information und Recht edition*. Verlag C. H. Beck, Munchen.

Heisenberg, D. (2005). *Negotiating privacy: The European Union, the United States, and personal data protection*. Boulder, USA: Lynne Rienner Publishers.

Jednak, S. (2017). Emerging Economies Development: BRICS vs East European Countries. *European Project Management Journal, 7(1)*, pp. 36-47.

Krivokapić, Đ., Krivokapić, D., Todorović, I., & Komazec, S. (2016). Mapping Personal Data Flow and Regulatory Compliance in Serbian Public Institutions. *Management - Journal of Sustainable Business and Management Solutions in Emerging Economies, 2016(80)*. pp. 1-10. DOI: 10.7595/management.fon.2016.0018.

Krivokapić, D., Krivokapić, Đ., Todorović, I., Komazec, S., Petrovski, A., & Ercegović, K. (2016). A Guide for Public Authorities – Personal Data Protection. SHARE Foundation, Novi Sad, Serbia. ISBN 978-86-89487-07-7.

Krivokapić, D., Krivokapić, Đ., Todorović, I., & Komazec, S. (2018). Impact of GDPR on Business: Focus on Data Controllers and Processors not Established within the EU. In Arsenijevic, O., Podbregar, I., Šprajc, P., Trivan, D., Ziegler, Y. (Eds.) *37th International Conference on Organizational Science Development: Organization and Uncertainty in the Digital Age*. University of Maribor, Faculty of Organizational Sciences, Kranj, Slovenia, pp. 527-539. DOI: https://doi.org/10.18690/978-961-286-146-9

Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. CRC Press, USA

Purtova, N. N. (2011). *Property rights in personal data: A European perspective*. Oisterwijk: BOX Press BV. Retrieved from https://pure.uvt.nl/ws/files/1312691/Purtova_property16-02-2011.pdf

Schwab, K., Marcus, A., Oyola, J. O., Hoffman, W., & Luzi, M. (2011). Personal data: The emergence of a new asset class. In *An Initiative of the World Economic Forum*.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security, 2016(6)*, 5-8. DOI: doi.org/10.1016/S1353-4858(16)30056-3

Todorović, I., Komazec, S., & Krivokapić, Đ. (2018). Key Roles and Activities in the Project of Business Compliance with GDPR. Proceedings of the XXII International Congress on Project Management: Business Agility and Agile Project Management.

Todorović, M., Petrović, D., Mihić, M., Obradović, V., & Bushuyev, S. (2015). Project success analysis framework: A knowledge-based approach in project management. *International Journal of Project Management, 33(4)*, pp. 772-783.

Venkataramanan, N., & Shriram, A. (2016). *Data Privacy: Principles and Practice*. CRC Press, USA.

Voigh, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer, USA.

Zarsky, T. Z. (2016). Incompatible: The GDPR in the Age of Big Data. *Seton Hall L. Rev., 47*, 995.